

משרד החינוך
המנהל הפדגוגי
אגף בכיר בחינוך
מחברת בחינה

לנבחנים ולנבחנות שלום,
יש לקרוא את ההוראות בעמוד זה ולמלא אותן בדיוקנות. אי-מילוי ההוראות עלול לגרום לתקלות ואף להביא לידי פסילת הבחינה.
הבחינה נועדה לבדוק הישגים אישיים, ולכן יש לעבוד עבודה עצמית בלבד. בזמן הבחינה אין להיעזר בזולת ואין לתת או לקבל חומר בכתב או בעל פה.
אין להכניס לחדר הבחינה חומר עזר – ספרים, מחברות, רשימות – חוץ מ"חומר עזר מותר בשימוש" המפורט בגוף השאלון או בהוראות מוקדמות של המשרד. כמו כן אין להכניס לחדר הבחינה טלפונים או מכשירים אלקטרוניים אחרים. שימוש בחומר עזר שאינו מותר יוביל לפסילת הבחינה.
לאחר סיום כתיבת הבחינה יש למסור את המחברת למשגיח ולעזוב בשקט את חדר הבחינה.

יש להקפיד על טוהר הבחינות !

הוראות לבחינה

- יש לוודא כי במדבקות הנבחן שקיבלת מודפסים הפרטים האישיים שלך. אין להוסיף או לשנות שום פרט במדבקות, כדי למנוע עיכוב בזיהוי המחברת וברישום הציונים.
- אם לא קיבלת מדבקה, יש למלא בכתב יד את הפרטים במקום המיועד למדבקת הנבחן.
- אסור לכתוב בשולי המחברת (החלק המקווקו) משום שחלק זה לא ייסרק.
- לטייטה ישמשו אך ורק דפי מחברת הבחינה שיועדו לכך.
- אין לתלוש או להוסיף דפים. מחברת שתוגש לא שלמה תעורר חשד לאי-קיום טוהר הבחינות.
- אין לכתוב שם בתוך המחברת משום שהבחינה נבדקת בעילום שם.

בהצלחה !

מדבקות נבחן והתאמות ملصقة ممتحن وملاءمات	מדבקות שאלון ملصقة نموذج امتحان
<div>שנה السنة חודש الشهر מועד موعد</div> <div>סמל ביה"ס מס' תעודת הזהות رقم المدرسة رقم الهوية</div>	
יש להדביק כאן ↑ מדבקות נבחן (ללא שם) يجب هنا ↑ إلصاق ملصقة ممتحن (بدون اسم)	
מדבקות לנבחן ملصقة ممتحن	

יש לסמן במשבצת ☐ אם ניתנה מחברת נוספת
يجب الإشارة في المربع إذا أُعطي دفتر إضافي
* التعليمات باللغة العربية على ظهر الصفحة

وزارة التربية والتعليم

القسم الكبير

الإدارة التربويّة
للامتحانات

دفتر امتحان

تحيّة للممتحنين وللممتحنات،
يجب قراءة التعليمات في هذه الصفحة والعمل وفقاً لها بدقة. عدم تنفيذ التعليمات قد يؤدي إلى عواقب مختلفة وحتى إلى إلغاء الامتحان. أعد الامتحان لفحص التحصيلات الشخصية، لذلك يجب العمل بشكل ذاتي فقط. أثناء الامتحان، لا يُسمح طلب المساعدة من الغير، ولا يُسمح إعطاء أو الحصول على مواد مكتوبة أو شفوية.
لا يُسمح إدخال مواد مساعدة - كتب، دفاتر، قوائم - إلى غرفة الامتحان، ما عدا "مواد مساعدة يُسمح استعمالها" المفصلة في نموذج الامتحان أو في تعليمات مسبقة من وزارة التربية والتعليم. كما لا يُسمح إدخال هواتف خلوية أو أجهزة إلكترونية أخرى إلى غرفة الامتحان. استعمال مواد مساعدة لا يُسمح استعمالها سوف يؤدي إلى إلغاء الامتحان.
بعد الانتهاء من كتابة الامتحان، يجب تسليم الدفتر للمراقب ومغادرة غرفة الامتحان بهدوء.

يجب التقيّد بنزاهة الامتحانات !

تعليمات للامتحان

1. يجب التأكّد بأنّ تفاصيلك الشخصية مطبوعة على ملصقات الممتحن التي حصلت عليها. لا يُسمح إضافة أو تغيير أية تفاصيل في الملصقات، وذلك لمنع عوائق في تشخيص الدفتر وفي تسجيل العلامات.
2. في حال عدم حصولك على ملصقة، يجب ملء التفاصيل في المكان المعدّ لملصقة الممتحن، بخط يد.
3. لا يُسمح الكتابة في هوامش الدفتر (في المنطقة المخططة)، لأنّه لن يتمّ مسح ضوئي لهذه المنطقة.
4. للمسوّدة تُستعمل أوراق دفتر الامتحان المعدّة لذلك فقط.
5. يُمنع نزع أو إضافة أوراق. الدفتر الذي يُسلم ناقصاً يُثير الشكّ بعدم الالتزام بنزاهة الامتحانات.
6. لا يُسمح كتابة الاسم داخل الدفتر، لأنّ الامتحان يُفحص بدون ذكر اسم.

نتمنّى لكم النّجاح!

מדינת ישראל

משרד החינוך

סוג הבחינה: גמר לבתי-ספר לטכנאים ולהנדסאים
מועד הבחינה: אביב תשפ"ד, 2024
סמל השאלון: 735913
נספח: מילון מונחים

יישומי ניתוב IP ואבטחה ברשתות קמפוס

הוראות לנבחנים

א. משך הבחינה: ארבע שעות ו-45 דקות.

ב. מבנה השאלון ומפתח ההערכה: בשאלון זה שני פרקים:

פרק ראשון: יישומי ניתוב IP	45 נקודות
פרק שני: אבטחה ברשתות קמפוס	55 נקודות
סך-הכול	100 נקודות

בשאלון זה שש שאלות. יש לענות על השאלות על-פי ההנחיות שבכל פרק.

ג. חומר עזר מותר בשימוש: מחשבון פשוט שאינו ניתן לתכנות ולא מאפשר להמיר ערכים בבסיסי ספירה שונים.
כל חומר עזר כתוב בכתב-יד או מודפס על נייר.

ד. הוראות מיוחדות:

- כתבו את כל התשובות בגוף השאלון, במקום המיועד לכך.
- כתבו בעט בלבד.
- עמודים 18–19 משמשים לטיוטה. כתיבת טיוטה בגוף השאלון או על דפים שמחוץ לשאלון עלולה לגרום לפסילת הבחינה.
- ענו על מספר הסעיפים הנדרש בכל פרק על-פי ההנחיות. המעריך יקרא ויעריך את מספר התשובות הנדרש בלבד לפי סדר כתיבתן, ולא יתייחס לתשובות נוספות.
- הדביקו את מדבקות הנבחן במקומות המיועדים לכך.
- בנספח לשאלון זה מובא מילון מונחים בשפות עברית, ערבית, אנגלית ורוסית. תוכלו להיעזר בו בעת הצורך.

שאלון זה משמש כמחברת בחינה. הדביקו את מדבקת הנבחן במקום המיועד לכך בעמוד 1 (כריכה קדמית).

בשאלון זה 20 עמודים ועמוד אחד של נספח.

השאלות בשאלון זה מנוסחות בלשון רבים, אף על פי כן על כל תלמידה וכל תלמיד להשיב עליהן באופן אישי.

בהצלחה!

המשך מעבר לדף

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

השאלות

בשאלון זה, כתבו את התשובות במקום המיועד לכך.
בשאלות רב-ברירה, לכל שאלה ארבע תשובות, אך רק אחת מהן נכונה. הקיפו את הספרה המציינת את התשובה הנכונה.
בשאלות האחרות, פעלו על-פי ההנחיות.

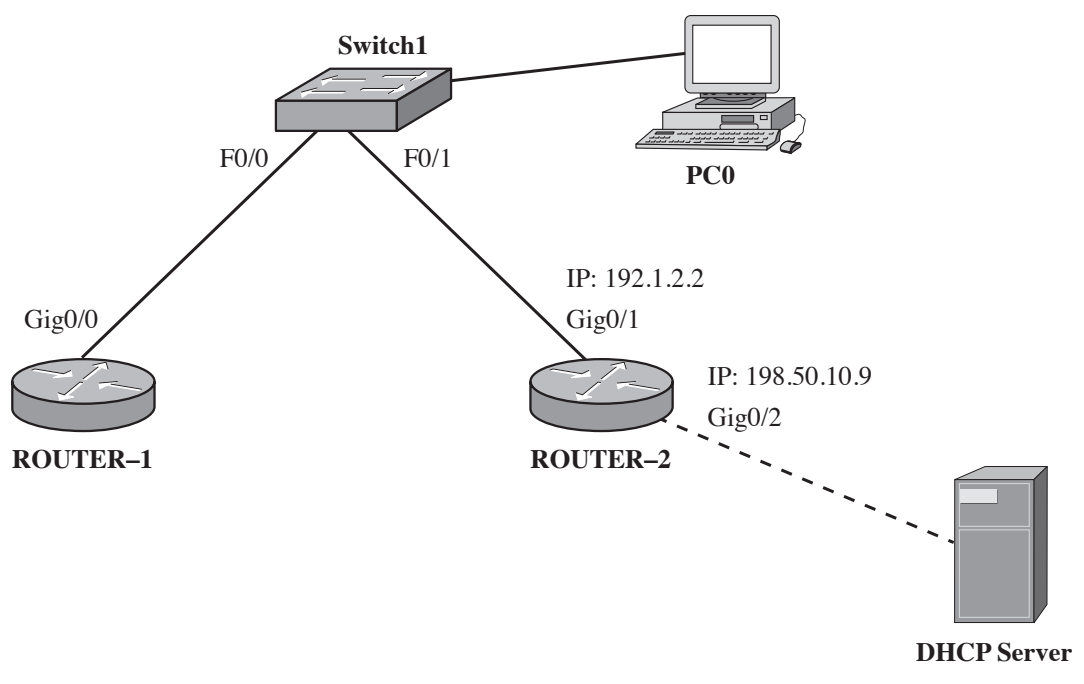
פרק ראשון: יישומי ניתוב IP (45 נקודות)

ענו על כל השאלות 1-3, על-פי ההנחיות (לכל שאלה – 15 נקודות).

שאלה 1

ענו על חמישה מבין הסעיפים א'-ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נק').

א. להלן טופולוגיה.



ההגדרות של המתג Switch1, שרת ה-DHCP והנתב Router-1 מלאות ותקינות.

השלימו את ההגדרות בנתב Router-2 כך שמחשב PC0 יוכל לקבל כתובת IP משרת DHCP.

Router-2(config)# interface Gig 0/1

Router-2(config-if)# _____

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ב. איזו פקודה מאפשרת לנתב להיהפך ללקוח DHCP?

1. ip address dhcp
2. ip helper-address
3. ip dhcp pool
4. ip dhcp client

ג. כיצד קובע הפרוטוקול EIGRP את מדד ברירת המחדל (default metric) של המסלול עבור טבלת הניתוב שלו?

1. הוא משתמש בערך 10 כמדד ברירת המחדל עבור כל המסלולים הנלמדים על ידי הנתב.
2. הוא מגדיר כמדד ברירת המחדל רק את מספר הדילוגים (hops) בין נתב המוצא לנתב היעד.
3. הוא משתמש בערכי רוחב הפס (bandwidth) וההשהיה (delay) של הנתב כדי לחשב את מדד ברירת המחדל של המסלול.
4. הוא מחשב את ההפרש בין רוחב הפס (bandwidth) לתפוקה (throughput) והערך המתקבל משמש כמדד ברירת המחדל.

ד. כתבו את ערך ה-Byte הראשון (8 סיביות) של הכתובת IPv6 – unique local address ברשת מקומית.

תשובה:

ה. בנתב Tikshuv נכתבו הפקודות הבאות:

```
Tikshuv(config) #router eigrp 130
Tikshuv(config-router) #network 10.4.3.0
Tikshuv(config-router) #network 172.16.4.0
Tikshuv(config-router) #network 192.168.2.0
Tikshuv(config-router) #auto-summary
```

אילו רשתות יתקבלו על ידי הנתבים השכנים?

1. 172.16.0.0 , 10.4.3.0 , 192.168.2.0
2. 172.16.4.0 , 10.0.0.0 , 192.168.0.0
3. 172.16.0.0 , 10.0.0.0 , 192.168.2.0
4. 172.16.4.0 , 10.4.3.0 , 192.168.2.0

ו. מה הסיבה להגדרת ממשק בנתב כ-*passive interface* בעת הגדרות ניתוב EIGRP?

1. הגדרת הממשק כממשק המועדף לקבלת תעבורה ועדכונים מנתבים שכנים
2. מניעה של לולאות ניתוב והפחתה של תעבורה ברשת
3. הגדרת ממשק גיבוי שיופעל אוטומטית בעת ניתוק ניתוב ברירת מחדל
4. מניעה של פרסום טבלאות ניתוב עודפות ועדכונים מנתבים שכנים

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

שאלה 2

ענו על חמישה מבין הסעיפים א'–ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נק').

א. לפניכם טבלה הכוללת תצורות שונות של מסיכות רשת (Subnet mask), מסיכות בדיקה (Wildcard mask) ו- CIDR (Classless Inter-Domain Routing).

השלימו את התאים הריקים בטבלה שלפניכם.

שימו לב, ה- Wildcard mask חייב להכיל את הטווח של כל הרשת.

CIDR	Wildcard mask	Subnet mask
	0.0.0.7	
/26		255.255.255.192
/8		255.0.0.0

ב. לפניכם רשימת פקודות שנכתבו בנתב Router:

```
ROUTER (config)#router ospf 1
ROUTER (config-router)#network 192.168.1.0 0.0.0.255 area 0
ROUTER (config-router)#ip ospf priority 10 192.168.1.0 0.0.0.255
```

מה המטרה של פקודות אלה?

1. תיעדוף של הניתוב לרשת יעד 192.168.1.0/24 על פני ניתובים אחרים לאותו היעד.
2. הגדרת ניתוב גיבוי לרשת יעד 192.168.1.0/24 עבור ניתובים אחרים לאותו היעד.
3. הגדרת ניתוב גיבוי לרשת יעד 192.168.0.0/24 עבור ניתובים אחרים לאותו היעד.
4. תיעדוף של הניתוב לרשת יעד 192.168.0.0/24 על פני ניתובים אחרים לאותו היעד.

ג. מנהל רשת הגדיר פרוטוקול EIGRP בנתב החברה, ופרסם את הרשתות הבאות:

10.1.1.0/24

10.1.2.0/24

10.1.3.0/24

10.1.4.0/24

כתבו את כתובת הרשת ואת ה- prefix שיפורסמו על-ידי הנתב לאחר שתבצע פעולת סכימת רשתות (route summarization).

תשובה:

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ד. מהו סוג ההודעה (message type) **שאינה שייכת** לפרוטוקול BGP?

1. KEEPALIVE
2. UPDATE
3. ACK
4. OPEN

ה. לפניכם ארבעה היגדים המתייחסים לפרוטוקולים BGP, OSPF, EIGRP.

קבעו לגבי כל אחד מן ההיגדים שלהלן אם הוא **נכון** או **לא נכון**, והקיפו בעיגול את התשובה הנכונה.

1. פרוטוקול BGP יודע לעבוד עם פרוטוקולים OSPF ו-EIGRP בלבד. **נכון / לא נכון**
2. פרוטוקול OSPF משתמש באלגוריתם DUAL כדי למנוע לולאות ניתוב. **נכון / לא נכון**
3. פרוטוקול EIGRP משתמש ב־HELLO packets כדי לעדכן את הנתבים השכנים לגבי קיומם ויכולותיהם. **נכון / לא נכון**
4. פרוטוקול EIGRP נחשב לבלתי אמין, מכיוון שהוא יכול להוביל למצב של לולאות (loops). **נכון / לא נכון**

ו. מנהל רשת הגדיר בנתב Router פרוטוקול ניתוב OSPF של אזור יחיד.

אחת מהרשתות שיפרסם הנתב היא 192.168.0.0, ומסיכת הרשת – 255.255.254.0.

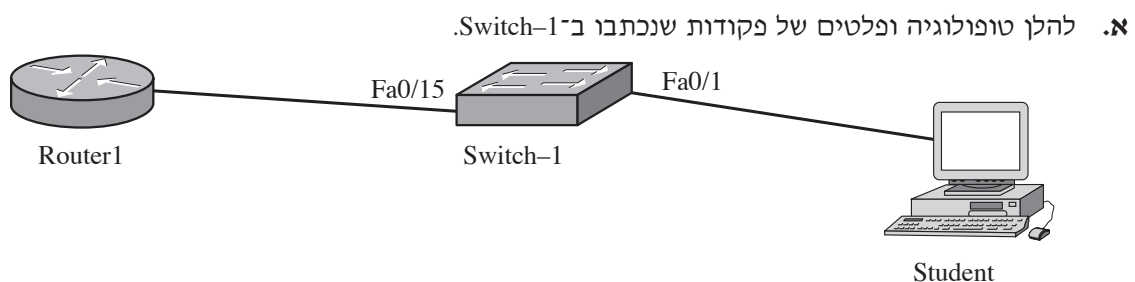
מהי מסיכת הבדיקה (Wildcard mask) שיש להגדיר לרשת זו?

תשובה: _____

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

שאלה 3

ענו על חמישה מבין הסעיפים א'-ו' על-פי ההנחיות שבכל סעיף (לכל סעיף - 3 נק').



פלט א'

```

Switch-1# show port-security interface Fa0/1
Port Security :Disabled
Port Status :Secure-down
Violation Mode :Restrict
Aging Time :0 mins
Aging Type :Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addresses : 0
Configure MAC Addresses : 0
Sticky MAC Addresses : 0
Last source Addresses:Vlan : 0000.0000.0000.0
Security Violation Count : 0
  
```

פלט ב'

```

Switch-1# show running-config interface Fa0/1
Building configuration...

Current configuration : 209 bytes
!
interface FastEthernet0/1
switchport access Vlan 5
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security mac-address sticky
  
```

מעוניינים לאפשר למחשב student **בלבד** להתחבר לממשק Fa0/1 במתג Switch-1. על-פי הפלטם, מה צריך להגדיר ב-Switch-1?

1. Port security במתג Switch-1 בכל הממשקים.
2. Port security במתג Switch-1 רק בממשק Fa0/1, ולאפשר בממשק זה חיבור אחד בלבד.
3. Vlan בממשק Fa0/1 כך שרק מחשב Student יוכל להתחבר אליו.
4. רשימת בקרת גישה (ACL) במתג בממשק Fa0/1, כך שרק מחשב Student יוכל להתחבר אליו.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

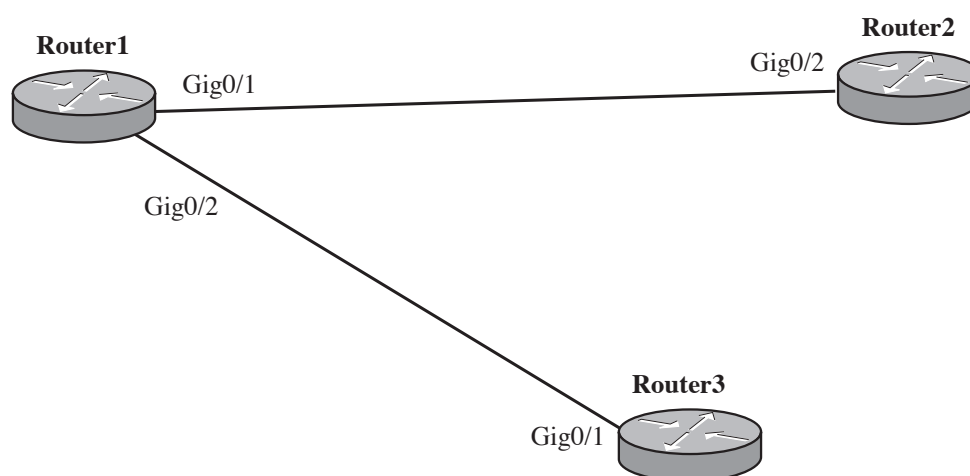
ב. בעת עבודה בפרוטוקול EIGRP, מהו סוג הניתוב שיוגדר כ-Feasible Successor והיכן הוא נשמר?

1. ניתוב ראשי (primary route), הנשמר בטבלת הניתוב (Routing Table).
2. ניתוב גיבוי (backup route), הנשמר בטבלת הניתוב (Routing Table).
3. ניתוב ראשי (primary route), הנשמר בטבלת הטופולוגיה (Topology Table).
4. ניתוב גיבוי (backup route), הנשמר בטבלת הטופולוגיה (Topology Table).

ג. מה תפקידו של נתב ABR בפרוטוקול הניתוב OSPF?

1. לחבר בין אזורים ב-OSPF.
2. לחבר בין OSPF ל-ISP.
3. להעביר חבילות בין פרוטוקול OSPF ל-EIGRP.
4. להעביר מנות VLSM.

ד. להלן טופולוגיה.



בנתב Router1 הוגדרו ההגדרות הבאות:

```
router ospf 1
passive-interface Gig0/1
```

מה יקרה כתוצאה מהגדרת הגדרות אלה בממשק Gig0/1 בנתב Router1?

1. יישלחו ויתקבלו חבילות hello, אך לא יישלחו חבילות LSAs.
2. לא יישלחו חבילות hello ולא יעובדו חבילות LSAs שהתקבלו.
3. לא יישלחו חבילות hello ולא יתקבלו בנתב עדכוני ניתוב מנתבים אחרים.
4. יתקבל ערך ה-cost הגבוה ביותר.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ה. כאשר קיימים כמה מסלולים בין נתב המקור לנתב היעד, איזה מסלול ייבחר על ידי הנתב?

1. המסלול עם חבילת התקשורת Monthly Usage הגבוהה ביותר.

2. המסלול עם העיכוב Latency הגבוה ביותר.

3. המסלול עם Administrative Distance הגבוה ביותר.

4. המסלול עם Administrative Distance הנמוך ביותר.

ו. מהי תדירות שליחת הודעות LSAs בפרוטוקול הניתוב OSPF? השלימו:

הודעות ה־LSA (בפרוטוקול OSPF) נשלחות בין הנתבים בכל _____ שניות.

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

פרק שני: אבטחה ברשתות קמפוס (55 נקודות)

ענו על כל השאלות 4–6, על-פי ההנחיות שבכל שאלה.

שאלה 4 (15 נקודות)

ענו על חמישה מבין הסעיפים א'–ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נק').

א. מנהל רשת זיהה כי שרת האינטרנט של החברה מקבל באופן חריג בקשות רבות לדפי אינטרנט ממקומות שונים בו זמנית. מהו סוג המתקפה האפשרית על רשת האינטרנט?

1. DDoS

2. phishing

3. social engineering

4. spyware

ב. תהליך הנפקת אישור דיגיטלי בשרת CA (Certification Authority) בנוי משלושה שלבים. בטבלה שלפניכם נתונים חמישה שלבים אפשריים של התהליך. זהו את שלושת השלבים הנכונים וכתבו בטבלה את מספרו של כל שלב לפי הסדר הנכון (1–3).

מספר השלב	תיאור השלב
	CA מנפיק אישור דיגיטלי עבור המשתמש או השירות
	המשתמש שולח בקשת DHCP Discovery לצורך איתור שרת CA
	המשתמש או השירות מבקש אישור דיגיטלי מ-CA
	CA מאמת את זהות המשתמש או השירות
	CA מפעיל תהליך אישור דיגיטלי באמצעות הפרוטוקול UDP

ג. בנתב Tikshuv-YD נכתבו הפקודות הבאות:

```
Tikshuv-YD(config)# access list 130 permit ip 192.168.5.0 0.0.0.255 10.10.2.0 0.0.0.255
```

```
Tikshuv-YD(config)# crypto map handesay 15 IPsec-isakmp
```

```
Tikshuv-YD(config-crypto-map)# match address 130
```

לנתב הגיעה חבילת נתונים מכתובת המקור 192.168.2.0, וכתובת היעד שלה היא 10.10.2.1.

מה יעשה הנתב עם חבילה זו?

1. ישלח אותה באופן מוצפן על ידי IPsec.

2. ידחה אותה ולא יאפשר את העברת החבילה.

3. ישלח אותה באופן לא מוצפן.

4. יעביר אותה לנתב השכן.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ד. מנהל רשת הגדיר בקרת אבטחה שנועדה להגביל את גישת המשתמשים לשרת FTP בלבד.

איזה רכיב במודל AAA יבצע הגדרה זו?

1. Accounting
2. Authentication
3. Authorization
4. Accessibility

ה. הפרוטוקול IPsec מספק בעיקר שירותי אימות והצפנה.

אילו שני פרוטוקולים מאפשרים זאת עבור IPsec?

1. Confidentiality ו- Authentication Header
2. Authentication Header ו- Encapsulating Security Payload (ESP)
3. Data Integrity ו- Internet Key Exchange
4. Encapsulating Security Payload (ESP) ו- Data Integrity

ו. לפניכם פקודות שהוגדרו בנתב Tikshuv.

```
Tikshuv(config)#aaa new-model
```

```
Tikshuv(config)#aaa authentication login default group tacacs+ local-case enable
```

מה יבצע הנתב Tikshuv בעת פעולת האימות מול שרת ה-?tacacs+

1. יפנה לשרת המוגדר. אם השרת אינו זמין יתבצע תהליך אימות מול הרשימה המקומית (login default group).
2. יפנה לרשימה המקומית (login default group). אם הרשימה אינה זמינה יתבצע תהליך אימות מול השרת המוגדר.
3. יאפשר למשתמשים בשרת tacacs+ גישה למצב enable ללא צורך בסיסמה, בתנאי שהם מוגדרים כמשתמשים מקומיים (local users).
4. ינסה לאמת את זהות המשתמש באמצעות מודל AES.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

שאלה 5 (20 נקודות)

ענו על חמישה מבין הסעיפים א'–ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 4 נק').

א. באיזה סוג מתקפה משתמשים במילון אלקטרוני כדי לגלות את סיסמת המערכת?

1. Buffer Overflow
2. Port Redirection
3. Denial of Service
4. Brute Force

ב. מה עלולה להיות ההשפעה של אי-ביצוע עדכוני אבטחה במערכת?

1. שמירה על יציבות ובדיקת ביצועי הרשת.
2. הגברת הסיכון לניצול פגיעויות מוכרות.
3. חיזוק של פרוטוקולי ההצפנה הא-סימטרית.
4. שיפור של אבטחת החומרה בהתקנים הקבועים של הרשת.

ג. איזה מהגורמים הבאים עלול לתרום לפגיעות ברשת עקב מעורבות אנושית?

1. הנדסה חברתית
2. גלישה דרך חומת אש
3. מדיניות סיסמאות חזקות
4. חולשות בפרוטוקולים ובתוכנה

ד. כדי למנוע מתקפה מסוימת בשכבת Data-Link, מנהל רשת השבית את הפרוטוקול

(Dynamic Trunking Protocol) DTP בכל הממשקים במתג.

מהו שם המתקפה שמנהל הרשת ניסה להתגונן מפניה?

תשובה:

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ה. איזה עיקרון של תקשורת מאובטחת מתממש בזכות הטמעת האלגוריתמים MD5 ו-SHA?

1. סודיות – Confidentiality
2. אימות – Authentication
3. שלמות – Integrity
4. ביקורת – Accounting

ו. מהן חמש הגדרות האבטחה שיש להגדיר במצב של תצורת מדיניות ISAKMP?

1. Hash, Authentication, GRE, Lifetime, ESP
2. Hash, Authorization, Group, Latency, Encryption
3. Hash, Accounting, Group, Lifetime, ESP
4. Hash, Authentication, Group, Lifetime, Encryption

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

שאלה 6 (20 נקודות)

ענו על חמישה מבין הסעיפים א'–ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 4 נק').

- א. לפניכם חמישה תיאורים אפשריים של תפקידי יחידות ה-BPDU. קבעו לגבי כל אחד מן התיאורים שלהלן אם הוא נכון או לא נכון, והקיפו בעיגול את התשובה הנכונה.

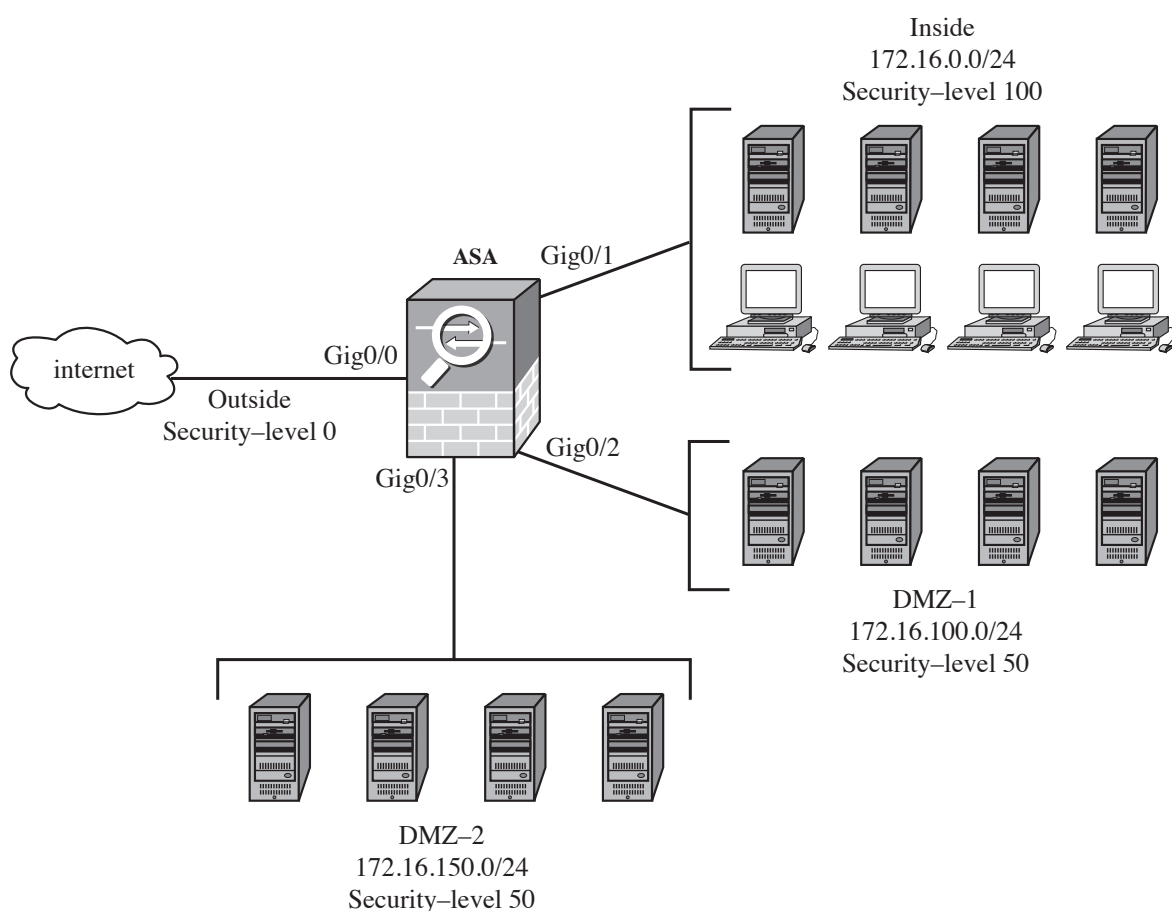
תיאור התפקיד	
לזהות את ה-Root Bridge	נכון / לא נכון
לחשב את ה-Root Bridge Cost	נכון / לא נכון
לזהות מתגים אחרים ברשת	נכון / לא נכון
לחשב את ה-port priority	נכון / לא נכון
לא לאפשר זיהוי של לולאות ניתוב ב-Vlans השונים	נכון / לא נכון

- ב. מתקפה מאיזה סוג משתמשת ב-packet flooding בחיבור TCP?

1. Brute Force
2. Trojan Horse
3. Reconnaissance
4. Denial of Service

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ג. להלן טופולוגיה של רשת.



נתון שלא הוגדרו כללים חריגים ב"חומת האש" (firewall). מה יאפשר התקן ה-ASA?

1. מנות שמקורן באינטרנט יוכלו להגיע לרשת 172.16.0.0/24 .
2. מנות שמקורן ברשת 172.16.100.0/24 יוכלו להגיע לרשת 172.16.0.0/24 .
3. מנות שמקורן ברשת 172.16.0.0/24 יוכלו להגיע לאינטרנט.
4. מנות שמקורן באינטרנט יוכלו להגיע לרשת 172.16.100.0/24 .

ד. בחברה מסוימת התרחש אירוע אבטחה. אחד העובדים חושד שמשתמש בלתי מורשה חדר למחשב שלו וטוען כי מהבוקר היישומים פועלים לאט ובצורה מוזרה. באיזה כלי של Microsoft Windows ניתן להיעזר כדי לקבוע אם ומתי מישהו נכנס למחשב במהלך הלילה?

1. Task Manager
2. PowerShell
3. Performance Monitor
4. Event Viewer

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

ה. מנהל רשת עדכן הגדרות אבטחה בממשק Gig 0/4 במתג Switch-1.
לפניכם הפלט שהוצג למנהל הרשת לאחר שכתב במתג את הפקודה show port-security interface Gig 0/4:

```
Port Security is enabled
Port Status is Secure-up
Violation Mode is Shutdown
Aging Time is 30 mins
Aging Type is Absolute
SecureStatic Address Aging is Disabled
Maximum MAC Addresses is 3
Total MAC Addresses is 2
Configured MAC Addresses is 1
Sticky MAC Addresses is 0
Last Source Address:Vlan is 0000.0C07.AC00.0001
Security Violation Count is 0
Switch-1#
```

על-פי הפלט, קבעו לגבי כל אחד מההיגדים שלהלן אם הוא **נכון** או **לא נכון**, והקיפו בעיגול את התשובה הנכונה.

1. הכתובת 0000.0C07.AC00.0001 זוהתה ככתובת חשודה. **נכון/לא נכון**
2. לא נרשמו עד כה הפרות אבטחה לממשק Gig 0/4. **נכון/לא נכון**
3. ממשק Gig 0/4 מאפשר לכל היותר ל-3 כתובות MAC להיות מחוברות אליו בו זמנית. **נכון/לא נכון**
4. הפרת אבטחה תגרום לממשק Gig 0/4 לעבור למצב כבוי באופן מיידי. **נכון/לא נכון**
5. ממשק Gig 0/4 מאובטח אך כרגע הוא במצב "לא פעיל". **נכון/לא נכון**

ו. מנהל הרשת בארגון מסוים קיבל הנחיה למנוע ממחשבים ברחבי הרשת לשלוח הודעות ICMP echo requests לשרת הארגון שכתובתו: 165.11.3.1 .
השלימו את הפקודה בהתאם להנחיה שלעיל.

access-list _____ icmp _____ 165.11.3.1 _____ eq echo

בהצלחה!

זכות היוצרים שמורה למדינת ישראל.
אין להעתיק או לפרסם אלא ברשות משרד החינוך.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

טיוטה

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب באזור זה

لا تكتب في هذه المنطقة

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ד, סמל 735913

טיוטה

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب באזור זה

لا تكتب في هذه المنطقة

מדבקת משגיח

ملصقة مراقب

"איתך בכל מקום, גם בבגרות.
בהצלחה, מועצת התלמידים והנוער הארצית"
"معك في كل مكان، وفي البجروت أيضًا.
بالنجاح، مجلس الطلاب والشبيبة القطري"

נספח: מילון מונחים
לשאלון 735913, אביב תשפ"ד

תרגום המונח			המונח
אנגלית	רוסית	ערבית	
פרק ראשון – יישומי ניתוב IP			
authentication	Идентификация	التَحْقُق	אימות
backup	Резервная копия	الحفظ الاحتياطي	גיבוי
topology table	Таблица топологии	جدول طوبولوجيا	טבלת טופולוגיה
routing table	Таблица маршрутизации	جدول توجيه	טבלת ניתוב
neighbors table	Таблица соседних элементов	جدول جيران	טבלת שכנים
routing loops	Петли маршрутизации	حلقات التوجيه	לולאות ניתוב
host	Хост-компьютер	مُضيف	מארח
packet	Пакет	وَجَبَة (دُفْعَة)	מנה
path	Путь	مسار	נתיב
server	Сервер	الخادم	שרת
פרק שני – אבטחה ברשתות קמפוס			
algorithm	Алгоритм	خوارزمية	אלגוריתם
encryption	Шифрование	تشفير	הצפנה
interface	Интерфейс	واجهة	ממשק
RSA key	RSA-ключ	مفتاح RSA	מפתח RSA
switch	Коммутатор/ Переключатель	مفتاح	מתג
router	Маршрутизатор	راوتر	נתב
port	Порт	مَنْفَذ	ממשק
protocol	Протокол	بروتوكول	פרוטוקול
access list	Список доступа	قائمة الوصول	רשימת גישה
network	Сеть	شبكة	רשת
configuration	Конфигурация	مواصفات	תצורה